重要インフラサイバーセキュリティ研究会（第２回）議事概要

１　日時

令和７年 12 月 22 日(月)16:00～18:00

２　場所

赤坂グリーンクロス４階　会議室

３　出席者

【構成員】

江崎　浩	東京大学大学院情報理工学系研究科教授
大日向　隆之	一般社団法人金融 ISAC 理事 株式会社三菱総合研究所エグゼクティブフェロー
柿崎　淑郎	東海大学情報通信学部准教授
北尾　辰也	国土交通省最高情報セキュリティアドバイザー
小松　文子	ノートルダム清心女子大学情報デザイン学部教授
小山　覚	NTT ドコモビジネス株式会社情報セキュリティ部部長
神保　謙	慶應義塾大学総合政策学部教授
長島　公之	公益社団法人日本医師会常任理事
西本　逸郎	株式会社ラック技術顧問
山岡　裕明	八雲法律事務所弁護士
渡辺　研司	名古屋工業大学大学院工学研究科社会工学専攻教授

【オブザーバ】

高見　穣	独立行政法人情報処理推進機構セキュリティセンター グループリーダー

４　議事概要

【議事】

（１）分野別ヒアリングについて

・事務局から、資料１に基づき、ヒアリング質問票について説明。

・電力分野、金融分野、水道分野及び医療分野のヒアリング対象の各担当者から、資料２、資料３、資料４及び資料５に基づき、ヒアリング質問票に対する回答についてそれぞれ説明。

（ヒアリング質問票に対する回答及びそれに関する質疑応答は非公開）

【主な発言】

〇構成員

・分野によっては、現場の人材不足により、遠隔監視や集中管理等の対策への依存が高まっていくものと思われる。このように、人員が不足すればするほどシステムの自動化が必要になり、サイバー攻撃のリスクも高まることを踏まえ、従来のセキュリティ対策の考えをシフトしなければならないという問題に留意する必要がある。

〇構成員

・これまで医療機関ではシステムを外部と繋がないようにすることで、サイバーセキュリティリスクを低減させていたが、国によりオンライン資格確認等システムの導入が義務化され、強制的に外部と接続することとなり、そのような環境に適したサイバーセキュリティ対策が必要となった。しかし小規模な医療機関をはじめ、ほとんどの医療機関では、知識・財源・人材の不足により、十分なセキュリティ対策を実施できておらず、大きな課題と認識している。

〇構成員

・近時発生したサイバー攻撃の事案において、被害の影響が他分野等に広く波及していることなどから、サプライチェーンのセキュリティ対策の重要性を改めて実感している。相互依存性の観点を踏まえ、重要インフラサービスに関連する他分野のサービスの防御についても留意する必要がある。

〇構成員

・セキュリティ人材の不足は分野共通の課題と思われる。この点は、例えば金融 ISAC では、人材育成プログラムやインテリジェンスの共有、演習等を実施しており、これらのような取組は人材不足に対する打ち手として考えられるのではないか。また、重要インフラ分野ごとに重視すべきサイバー攻撃のクリティカルなシナリオが異なるものと思われる。この点は、セプター等ごとに重視すべきシナリオを整理していくことにより、対策の質が向上するのではないか。

〇構成員

・各分野で共通する取組、例えば人材育成、人手の派遣、研修等について、分野を超え、あるいは地域間で連携して実施できるようになると望ましいのではないか。また、各分野の特性を明らかにすることにより、自らの分野で実施すべき取組が把握できるほか、ある分野の特性が他の分野にとっても参考になることもあり得る。このように、重要インフラ統一

基準においては、各分野の連携を促進するといった観点で作成していただきたい。

（2）その他

【主な発言】

〇構成員

・各重要インフラ分野における特性・実情・課題等を把握する観点から、安全基準等により実施が求められているセキュリティ対策と、実際に各事業者において実施できているセキュリティ対策とは区別して調査していく必要がある。

〇構成員

・安易に専用 OS であればセキュリティが確保されると思っているのであれば、危機感を持つべきである。このように、各分野のリスクアセスメントの中で、共通して抜けているものについてより注意すべきである。

〇構成員

・重要インフラ統一基準を策定する際の視点として、「標準化」が１つのポイントになると考えている。TPRM(サードパーティリスク管理)について、各社が独自に策定したルールを委託先に強いることにより、委託先の負担が増加し破綻する事例が多い。委託元も管理が困難となっている。TPRM の標準化を行うことができれば、各事業者の負担が軽減され、利便性も高まるのではないか。

・多要素認証の導入は普及しつつある一方、それを組織内で徹底できているかという点、凡事徹底が重要である。業界として重要な IT システムについては、多要素認証をデフォルト化することも一案。

・クラウドの利活用の推進についても検討すべきである。脆弱性対策やバックアップ等をクラウドベンダー側が管理するサービスを選べば、ユーザーの負担が軽減される。また、中小企業等では、クラウドの利活用により、セキュリティ対策のコストが軽減される場合もある。さらに、クラウド環境ではバックアップも堅牢であるところ、公表事例ベースではクラウド環境でデータが暗号化被害を受けたランサムウェア事案は確認しておらず、少ないのではないか。

〇構成員

・クラウドの利活用について、クラウド事業者がサイバー攻撃を受けた場合、非常に大きな被害が生じる可能性があるため、クラウドを利用する場合の基準について慎重に検討する必要がある。

〇構成員

・いわゆる閉域網神話について、仮に現時点で閉域網だとしても、将来的に外部のネットワークと接続した場合、セキュリティを取り巻く環境が大きく変わっているため、必要な技術的知見等が不足しており対応できないのではないかという懸念がある。マイナスからスタートするイメージである。このような観点から、最先端の対策に留意しつつも、基本的対策の徹底が最も重要だと考える。

〇構成員

・閉域網は安全ではない。例えば、閉域網として構築した環境のインターネット境界面のネットワーク機器が侵害され、攻撃を受けることもある。近年、国家を背景とする攻撃者をはじめとして、ネットワーク機器を起点としたサイバー攻撃が発生しているところ、この点について正確な情報が流通していないように思われる。事業者に対し、セキュリティ・クリアランス制度等も活用しつつ、サイバー攻撃に関する情報を正しく伝え、対策を促していくことを検討いただきたい。

〇構成員

・ゼロトラストが重要であるところ、閉域網において専用 OS を使用していれば安全といったような安易な考えを戦略的に変えていく必要がある。このような動きは業界間で差が大きく、例えば、グローバルマーケットで勝負している半導体業界は、セキュリティの取組を強固に推進している。このような業界としての意思決定を政府がどのように政策としてドライブしていくかや、業界としてのベストプラクティス等をどのように共有・導入していくかについては、知恵を絞る必要がある。

【今後の予定】

・事務局から、次回の研究会の開催予定について説明。